DEPARTMENT OF THE ARMY
MILITARY SURFACE DEPLOYMENT AND DISTRIBUTION COMMAND
200 STOVALL STREET
ALEXANDRIA, VA 22332-5000

SDG6 13 Aug 04

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Policy for Removable Storage Media (Flash/Pen Drives)

1. References:

a. AR 25-1, Chapter 5, Information Assurance, 31 May 2002

b. AR 25-2, Chapter 4, Information Assurance Policy, 14 November 2003

c. AR 380-5, Chapter 4, Information Security Program, 29 September 2000

d. AR 190-13, Chapter 5, Army Physical Security Program, 30 September 1993

2. New technologies in secondary storage media have made it necessary to clarify current Information Assurance and Physical Security policy, as these devices may pose additional risk to SDDC systems or could cause unintended compromise of restricted information. Operational benefits of highly portable, reusable and removable secondary storage media devices are acknowledged. This policy refers to any device that can be connected to a workstation, server, or other computing component via cable or universal serial bus (USB).

3. A new family of media storage devices has evolved. Most notably among these is the Flash/Pen Drive. Users can take unclassified work home with them, or travel with just their data instead of lugging a laptop around. Documents can be edited and data can be repeatedly stored on Flash/Pen Drives. Administrators and support personnel can use Flash/Pen Drives as a portable toolkit that includes recovery tools, drivers, system updates, and diagnostic utilities. Files can be backed up to the Flash/Pen Drive before editing live versions.

4. Because these devices have no moving parts, they're more durable than other forms of removable media. The Flash/Pen Drive's small size and large storage capacity make it a dangerous tool in the wrong hands and present two primary threats to SDDC network and workstations as well as the physical control of restricted data. These include the introduction of malicious software code and the theft or loss of data.

5. Government-procured and issued removable secondary storage media devices of any capacity are approved for use in NIPRNET computer systems. Due to the inherent risk, posed by secondary storage media to include Flash/Pen drives to national defense information, the following procedures are established:

a. Labeling. All removable secondary storage media **will be** labeled in accordance with AR 380-5, indicating the highest classification or sensitivity of the data contained on the device. Generally, any identification will follow standard marking convention for unclassified and classified data. The color green will be for unclassified and red for classified. Originators must mark both internal media labels and internal files with the highest classification of data the media contains. If the device is too small, then a SDDC approved color-coded identification card/label will be attached to the media. Additionally, the device will be marked with a permanent marker or other form of identification indicating the classification level and, when not in use, stored in an approved security container.

b. Information **will not** be permanently stored on Flash/Pen Drives. The Flash/Pen Drive will be used primarily to transport files between workstations or servers. They will be used for the duration of the required transport and the information will be deleted from the Flash/Pen Drive when the procedure is completed.

c. Flash/Pen Drives used at home or on non-government systems **will be scanned** by G6 personnel or G6 designated personnel for malicious code prior to use on government systems.

d. Flash/Pen Drives **will not** be used interchangeably on the NIPRNET and SIPRNET.

e. Flash/Pen Drives **will** be formatted for New Technology File System (NTFS) prior to use. NTFS files are not accessible from other operating systems and are the recommended format for Flash/Pen Drives.

f. If a Flash/Pen Drive becomes inoperable, individuals **will** contact the G6 for assistance before proceeding further with the use of the drive.

g. Removable storage media of any type for classified material **will not** be issued without a courier designation and the possession of an official courier card. The security manager under G2 remains the proponent for designation. Devices designated for classified information, empty or otherwise, will not leave the work center, unless in an official courier capacity.

6. Personally owned removable storage media, to include Flash/Pen Drives, **will not** be used on the SIPRNET unless specifically approved in writing by the Information Assurance Manager (IAM) or the Designated Approval Authority (DAA). Owners of devices approved for SIPRNET application will be specifically trained in their use by IM and briefed regarding security requirements by G2. Government owned devices will be controlled as follows:

a. Taken under administrative control by G6 and issued to users as required.

b. Will not be indiscriminately carried on one's person out of the work area.

c. Any drive is subject to random inspection by G2 or G6 staff for compliance with security directives.

d. Small drives will be worn in a conspicuous location in order to be readily seen when transporting within the work center.

e. Inoperable/malfunctioning devices will be returned to G6 for evaluation, repair or destruction.

7. Administrative requirements specified herein for the control and use of Flash/Pen Drives are mandatory. The provisions of AR 380-5, Chapter 1, Section VII, Corrective Actions and Sanctions, and Chapter 10, Section 1, Unauthorized Disclosure and Other Security Incidents, will apply.

8. The G6 points of contacts are Mr. Albert Fraser at the OPS Center, (757) 878-7497 and Mr. Don Carter at Alexandria, (703) 428-2171. Security manager point of contact is Alton Stowell, 757-878-8416.

E-Signed by SDDC User John Smith
Verify authenticity with ApproveIt
John S. Smith

John S. Smith
Deputy Chief of Staff, G6

DISTRIBUTION:
Director, SDDC Transportation Engineering Agency, 720 Thimble Shoals Blvd, Suite 130,
Newport News, VA 23606-2574
Commander, 597th Transportation Group, Military Ocean Terminal Sunny Point,
6280 Sunny Point Road, Southport, NC 28461-5000
Commander, 598th Transportation Group, Unit 6713, Box 173, APO AE 09709
Commander, 599th Transportation Group, Bldg 204, Wheeler AAF, Schofield Barracks,
HI 96857-5008
HQ SDDC Staff Principals